EXHIBIT 4

United States of America
FEDERAL TRADE COMMISSION
BUREAU OF CONSUMER PROTECTION
600 PENNSYLVANIA AVENUE NW, CC-9528
WASHINGTON, DC 20580

Reenah L. Kim
Division of Enforcement
(202) 326-2272
rkim1@ftc.gov

August 31, 2022

VIA ELECTRONIC MAIL

Lydia Parnes, Esq. (lparnes@wsgr.com)
Eddie Holman, Esq. (eholman@wsgr.com)
Brett Weinstein, Esq. (bweinstein@wsgr.com)
Wilson Sonsini Goodrich & Rosati
1700 K Street, NW, Fifth Floor
Washington, DC 20006

Re: *In the Matter of Twitter, Inc.*, Docket No. C-4316

Dear Counsel:

As you know, former Twitter employee Peiter "Mudge" Zatko has made numerous claims regarding deficiencies in the Company's privacy, security, and integrity measures.[1] Specifically, Zatko alleges Twitter never achieved "full compliance" with the Federal Trade Commission ("FTC" or "Commission")'s March 2, 2011, consent order ("2011 Order").[2]

We take these issues very seriously. Accordingly, pursuant to Part XIII of the Commission's May 26, 2022, Order in the above-referenced matter ("2022 Order"), we ask that Twitter submit by **September 14, 2022**, a true and accurate written report, sworn under penalty of perjury, containing responses to the following requests:

1. Zatko states that in or about August 2021, he notified then-CTO Parag Agrawal and others that the login system for Twitter's engineers was registering, on average, 1,500 and 3,000 failed logins every day, which Zatko considered to be "a huge red flag." He

[1] *See, e.g.,* "Former Security Chief Claims Twitter Buried 'Egregious Deficiencies,'" Aug. 23, 2022, *Washington Post*.

[2] *See* July 6, 2022 Whistleblower Disclosure ¶ 46, *available at* https://www.washingtonpost.com/technology/interactive/2022/twitter-whistleblower-sec-spam/?document=undefined ("Zatko Disclosure").

further states Agrawal "acknowledged that no one knew that, and never assigned anyone to diagnose why this was happening or how to fix it." Zatko Disclosure ¶64.

a. State whether You[3] agree or disagree with these assertions, specifying which parts of these statements You believe are or have been accurate at any time. To the extent You contend any practice, policy, procedure, gap, weakness, or deficiency referenced in these statements existed at one time, but is no longer occurring or no longer exists, please clarify the applicable time periods and describe the circumstances in which the conduct ceased.

b. If You disagree, whether in whole or in part, explain why and provide the complete basis for Your response.

c. If You agree, whether in whole or in part, state whether Your failure to address thousands of failed login attempts every day is consistent with Your obligation to establish, implement, and maintain a comprehensive privacy and information security program that protects the privacy, security, confidentiality, and integrity of Covered Information under the Order, and if so, explain how it is consistent.

    i. As part of Your response, describe what You did to address the issue of the high volume of failed logins for the system used by Twitter engineers.

2. Zatko states that over the course of 2021, he became aware of multiple episodes suggesting Twitter had been "penetrated by foreign intelligence agencies." Specifically, Zatko states the Indian government "forced Twitter to hire specific individual(s) who were government agents, who . . . would have access to vast amounts of sensitive Twitter data." Zatko Disclosure ¶72.a.

a. State whether You agree or disagree with these assertions, specifying which parts of these statements You believe are or have been accurate at any time. To the extent You contend any practice, policy, procedure, gap, weakness, or deficiency referenced in these statements existed at one time, but is no longer occurring or no longer exists, please clarify the applicable time periods and describe the circumstances in which the conduct ceased.

b. If You disagree, whether in whole or in part, explain why and provide the complete basis for Your response.

c. If You agree, whether in whole or in part, state whether Your hiring of Indian government agents as Twitter employees with access to sensitive Twitter data is consistent with Your obligation to establish, implement, and maintain a

[3] For purposes of these requests, "You" and "Your" shall mean Twitter, Inc., its successors and assigns, and any business it controls directly or indirectly, and all directors, officers, members, employees, agents, consultants, and other persons working for or on behalf of the foregoing.

comprehensive privacy and information security program that protects the privacy, security, confidentiality, and integrity of Covered Information under the Order, and if so, explain how it is consistent.

3. Zatko states that, shortly before he was terminated in January 2022, Twitter received "specific information from a U.S. government source that one or more particular Company employees were working on behalf of another particular foreign intelligence agency." Zatko Disclosure ¶72.e.

   a. State whether You agree or disagree with these assertions, specifying which parts of these statements You believe are or have been accurate at any time. To the extent You contend any practice, policy, procedure, gap, weakness, or deficiency referenced in these statements existed at one time, but is no longer occurring or no longer exists, please clarify the applicable time periods and describe the circumstances in which the conduct ceased.

   b. If You disagree, whether in whole or in part, explain why and provide the complete basis for Your response.

   c. Describe in detail the alleged information received from the U.S. government source.

   d. If You agree, whether in whole or in part, state whether Your hiring and retention of Company employees who were also working on behalf of another nation's foreign intelligence agency is consistent with Your obligation to establish, implement, and maintain a comprehensive privacy and information security program that protects the privacy, security, confidentiality, and integrity of Covered Information under the Order, and if so, explain how it is consistent.

4. Zatko states that Twitter "employee computers are exposed, with over 30% of devices reporting they had disabled software and security updates." Zatko further states that "a large portion of employee computers" had "system firewalls turned off, and remote desktop enabled for non-approved purposes." Zatko Disclosure ¶46.b.ii.n.54.

   a. State whether You agree or disagree with these assertions, specifying which parts of these statements You believe are or have been accurate at any time. To the extent You contend any practice, policy, procedure, gap, weakness, or deficiency referenced in these statements existed at one time, but is no longer occurring or no longer exists, please clarify the applicable time periods and describe the circumstances in which the conduct ceased.

   b. If You disagree, whether in whole or in part, explain why and provide the complete basis for Your response.

   c. If You agree, whether in whole or in part, state whether Your allowing employees to disable software and security updates on their computers, turn off system

firewalls, and enable remote desktop for non-approved purposes is consistent with Your obligation to establish, implement, and maintain a comprehensive privacy and information security program that protects the privacy, security, confidentiality, and integrity of Covered Information under the Order, and if so, explain how it is consistent.

i. As part of Your response, describe the circumstances in which Twitter employees were or are allowed to disable software and security updates, turn off system firewalls, and/or enable remote desktop for non-approved purposes, and explain why You allow(ed) this to occur. In addition, describe any technical controls You implemented to prevent employees from deviating from Your policy.

d. State how many Twitter employee computers are not running the latest version of the operating system provided by the vendor(s) used by Twitter, and explain why they are not running the latest version. Please provide this figure as an absolute number and as a percentage of the total number of employee computers.

e. State how many Twitter employee computers have the macOS System Integrity Protection (SIP) feature disabled, and explain why those devices have SIP disabled. Please provide this figure as an absolute number and as a percentage of the total number of employee computers running macOS.

5. Zatko states "Twitter did not actively monitor what employees were doing on their computers. Although against policy, it was commonplace for people to install whatever software they wanted on their work systems," and Twitter employees "were repeatedly found to be intentionally installing spyware on their work computers at the request of external organizations. Twitter learned of this several times only by accident, or because of employee self-reporting." Zatko Disclosure ¶46.b.ii.n.54.

a. State whether You agree or disagree with these assertions, specifying which parts of these statements You believe are or have been accurate at any time. To the extent You contend any practice, policy, procedure, gap, weakness, or deficiency referenced in these statements existed at one time, but is no longer occurring or no longer exists, please clarify the applicable time periods and describe the circumstances in which the conduct ceased.

b. If You disagree, whether in whole or in part, explain why and provide the complete basis for Your response.

c. If You agree, whether in whole or in part, state whether Your allowing employees to install whatever software they wanted on their work systems, including spyware, is consistent with Your obligation to establish, implement, and maintain a comprehensive privacy and information security program that protects the privacy, security, confidentiality, and integrity of Covered Information under the Order, and if so, explain how it is consistent.

i. As part of Your response, describe the circumstances in which Twitter employees were or are allowed to install whatever software they wanted on their work systems, including spyware, and explain why You allow(ed) this to occur. In addition, describe any technical controls You implemented to prevent employees from deviating from Your policy.

6. Zatko states that Twitter had "no mobile device management (MDM) for employee phones, leaving the Company with no visibility or control over thousands of devices used to access core company systems." Zatko Disclosure ¶46.b.iii.

a. State whether You agree or disagree with these assertions, specifying which parts of these statements You believe are or have been accurate at any time. To the extent You contend any practice, policy, procedure, gap, weakness, or deficiency referenced in these statements existed at one time, but is no longer occurring or no longer exists, please clarify the applicable time periods and describe the circumstances in which the conduct ceased.

b. If You disagree, whether in whole or in part, explain why and provide the complete basis for Your response.

c. If You agree, whether in whole or in part, state whether Your lack of mobile device management for employee phones is consistent with Your obligation to establish, implement, and maintain a comprehensive privacy and information security program that protects the privacy, security, confidentiality, and integrity of Covered Information under the Order, and if so, explain how it is consistent.

d. As part of Your response, describe the types of access that unmanaged employee phones had to Twitter's systems and user data, and explain why You allow(ed) this to occur.

7. Zatko states that in or around Q3-Q4 2021, he learned that "no Twitter employee computers were being backed up at all," and that although Twitter's IT department had purportedly managed a backup system for years, it had never been tested and was not functioning correctly, raising the risks for corporate data integrity." Zatko Disclosure ¶65.

a. State whether You agree or disagree with these assertions, specifying which parts of these statements You believe are or have been accurate at any time. To the extent You contend any practice, policy, procedure ,gap, weakness, or deficiency referenced in these statements existed at one time, but is no longer occurring or no longer exists, please clarify the applicable time periods and describe the circumstances in which the conduct ceased.

b. If You disagree, whether in whole or in part, explain why and provide the complete basis for Your response.

c. If You agree, whether in whole or in part, state whether Your lack of employee computer backups is consistent with Your obligation to establish, implement, and maintain a comprehensive privacy and information security program that protects the privacy, security, confidentiality, and integrity of Covered Information under the Order, and if so, explain how it is consistent.

i. As part of Your response, describe the circumstances in which Twitter employees kept production data on their laptops (e.g., systemic or a one-off ad-hoc arrangement), and explain why You allow(ed) this to occur. In addition, describe any technical or other controls You implemented to prevent employees from deviating from Your policy or standard practice.

8. Zatko states Twitter did not have a means for sealing its production environment. Specifically, he states that during the January 6th Capitol Attack, he asked the executive in charge of engineering how the Company could seal the production environment to "protect the integrity and stability of the service from a rogue or disgruntled engineer." According to Zatko, he learned "it was impossible to protect the production environment," since all engineers had access. Moreover, "[t]here was no logging of who went into the environment or what they did. . . . There were no logs, nobody knew where data lived or whether it was critical, and all engineers had some form of critical access to the production environment." Zatko Disclosure ¶48.

a. State whether You agree or disagree with these assertions, specifying which parts of these statements You believe are or have been accurate at any time. To the extent You contend any practice, policy, procedure, gap, weakness, or deficiency referenced in these statements existed at one time, but is no longer occurring or no longer exists, please clarify the applicable time periods and describe the circumstances in which the conduct ceased.

b. If You disagree, whether in whole or in part, explain why and provide the complete basis for Your response.

c. If You agree, whether in whole or in part, state whether Your allowing broad employee access to the production environment and/or lack of logging is consistent with Your obligation to establish, implement, and maintain a comprehensive privacy and information security program that protects the privacy, security, confidentiality, and integrity of Covered Information under the Order, and if so, explain how it is consistent.

9. Zatko alleges "ignorance and misuse of vast internal data sets, with only about 20% of Twitter's huge data sets registered and managed." Zatko Disclosure ¶46.a.i.

a. State whether You agree or disagree with these assertions, specifying which parts of these statements You believe are or have been accurate at any time. To the extent You contend any practice, policy, procedure, gap, weakness, or deficiency

referenced in these statements existed at one time, but is no longer occurring or no longer exists, please clarify the applicable time periods and describe the circumstances in which the conduct ceased.

b. If You disagree, whether in whole or in part, explain why and provide the complete basis for Your response.

c. If You agree, whether in whole or in part, state whether Your deficient data-lineage understanding and management is consistent with Your obligation to establish, implement, and maintain a comprehensive privacy and information security program that protects the privacy, security, confidentiality, and integrity of Covered Information under the Order, and if so, explain how it is consistent.

10. Zatko states that in January 2022, he determined Twitter had over 300 corporate systems and more than 10,000 services that might still be affected by the "Log4j" software vulnerability because of "poor engineering architecture decisions." Zatko further states Twitter was "unable to thoroughly assess its exposure to Log4j, and did not have capacity, if pressed in a formal investigation, to show to the FTC that the Company had properly remediated the problem." Zatko Disclosure ¶69.

a. State whether You agree or disagree with these assertions, specifying which parts of these statements You believe are or have been accurate at any time. To the extent You contend any practice, policy, procedure, gap, weakness, or deficiency referenced in these statements existed at one time, but is no longer occurring or no longer exists, please clarify the applicable time periods and describe the circumstances in which the conduct ceased.

b. If You disagree, whether in whole or in part, explain why and provide the complete basis for Your response.

c. If You agree, whether in whole or in part, state whether Your inability to fully demonstrate Your remediation of the Log4j vulnerability is consistent with Your obligation to establish, implement, and maintain a comprehensive privacy and information security program that protects the privacy, security, confidentiality, and integrity of Covered Information under the Order, and if so, explain how it is consistent.

d. Describe in detail the process by which Twitter sought to remediate the Log4j vulnerability.

i. As part of Your response, explain whether and how You addressed the scanning of source code and product infrastructure.

ii. As part of Your response, specify the time periods when remediation work was commenced and completed.

iii. Describe the extent to which any residual risk associated with the Log4j vulnerability relates to third-party products or services You deploy, as compared to the extent to which any residual risk concerns software developed by Twitter.

11. Zatko states that Twitter had "server vulnerabilities, with over 50% of Twitter's 500,000 data center servers with non-compliant kernels or operating systems, and many unable to support encryption at rest." Zatko Disclosure ¶46.b.i.

a. State whether You agree or disagree with these assertions, specifying which parts of these statements You believe are or have been accurate at any time. To the extent You contend any practice, policy, procedure, gap, weakness, or deficiency referenced in these statements existed at one time, but is no longer occurring or no longer exists, please clarify the applicable time periods and describe the circumstances in which the conduct ceased.

b. If You disagree, whether in whole or in part, explain why and provide the complete basis for Your response.

c. If You agree, whether in whole or in part, state whether the existence of these server vulnerabilities is consistent with Your obligation to establish, implement, and maintain a comprehensive privacy and information security program that protects the privacy, security, confidentiality, and integrity of Covered Information under the Order, and if so, explain how it is consistent.

12. Zatko states Twitter failed to implement a Software Development Life Cycle (SDLC), a "uniform process to develop and test software, and a basic best practice for engineering development at commercial companies." Zatko further states the Company had been reporting regularly to the Board that the SDLC effort was "getting closer to being complete," when in fact the Company only had "a template for the SDLC, not even a functioning process," and that "by Q2 2021 that template had only been rolled out for roughly 8-12% of projects." Zatko Disclosure ¶¶58-59.

a. State whether You agree or disagree with these assertions, specifying which parts of these statements You believe are or have been accurate at any time. To the extent You contend any practice, policy, procedure, gap, weakness, or deficiency referenced in these statements existed at one time, but is no longer occurring or no longer exists, please clarify the applicable time periods and describe the circumstances in which the conduct ceased.

b. If You disagree, whether in whole or in part, explain why and provide the complete basis for Your response.

c. If You agree, whether in whole or in part, state whether Your lack of a fully implemented SDLC process is consistent with Your obligation to establish, implement, and maintain a comprehensive privacy and information security

program that protects the privacy, security, confidentiality, and integrity of Covered Information under the Order, and if so, explain how it is consistent.

13. Zatko states Twitter lacked appropriate development and testing environments for all software development and testing, which he characterized as "highly anomalous for a large tech company." Specifically, Zatko states that Twitter engineers "built, tested, and developed new software directly in production with access to live customer data and other sensitive information in Twitter's system," which reflects a "lack of basic engineering hygiene." Zatko Disclosure ¶46.c.i.n.57.

    a. State whether You agree or disagree with these assertions, specifying which parts of these statements You believe are or have been accurate at any time. To the extent You contend any practice, policy, procedure, gap, weakness, or deficiency referenced in these statements existed at one time, but is no longer occurring or no longer exists, please clarify the applicable time periods and describe the circumstances in which the conduct ceased.

    b. If You disagree, whether in whole or in part, explain why and provide the complete basis for Your response.

    c. If You agree, whether in whole or in part, state whether Your lack of appropriate software development and testing environments separate from Your live production environment is consistent with Your obligation to establish, implement, and maintain a comprehensive privacy and information security program that protects the privacy, security, confidentiality, and integrity of Covered Information under the Order, and if so, explain how it is consistent.

* * * * *

Please have a responsible corporate officer or manager of Twitter certify under penalty of perjury that the written report(s) submitted in response to this letter is complete and accurate, and that the report and accompanying document production(s) represent all information responsive to the FTC's requests.

All information provided in response to these requests must be submitted in an electronic format agreed upon by a Commission representative in writing prior to the submission. So that the FTC has the capability of reading and using the data, please ensure that the submission of Electronically Stored Information ("ESI") complies with the attached Production Instructions, and contact us in advance to arrange for the electronic submission of materials via SFTP. Please send an electronic copy of your responses to the Commission at DEBrief@ftc.gov, with copies to rkim1@ftc.gov.

Finally, Twitter should suspend any routine procedures for document destruction and take other measures to preserve all records relating to the matters addressed in this letter, including electronically stored records that are stored on backup media and all physical records stored offsite, in a form that includes the complete record.

Sincerely,

Reenah L. Kim

cc: Gustav W. Eyler, USDOJ
Lisa K. Hsiao, USDOJ
Zachary L. Cowan, USDOJ
Deborah S. Sohn, USDOJ